KPMG

Una triple amenaza en las Américas

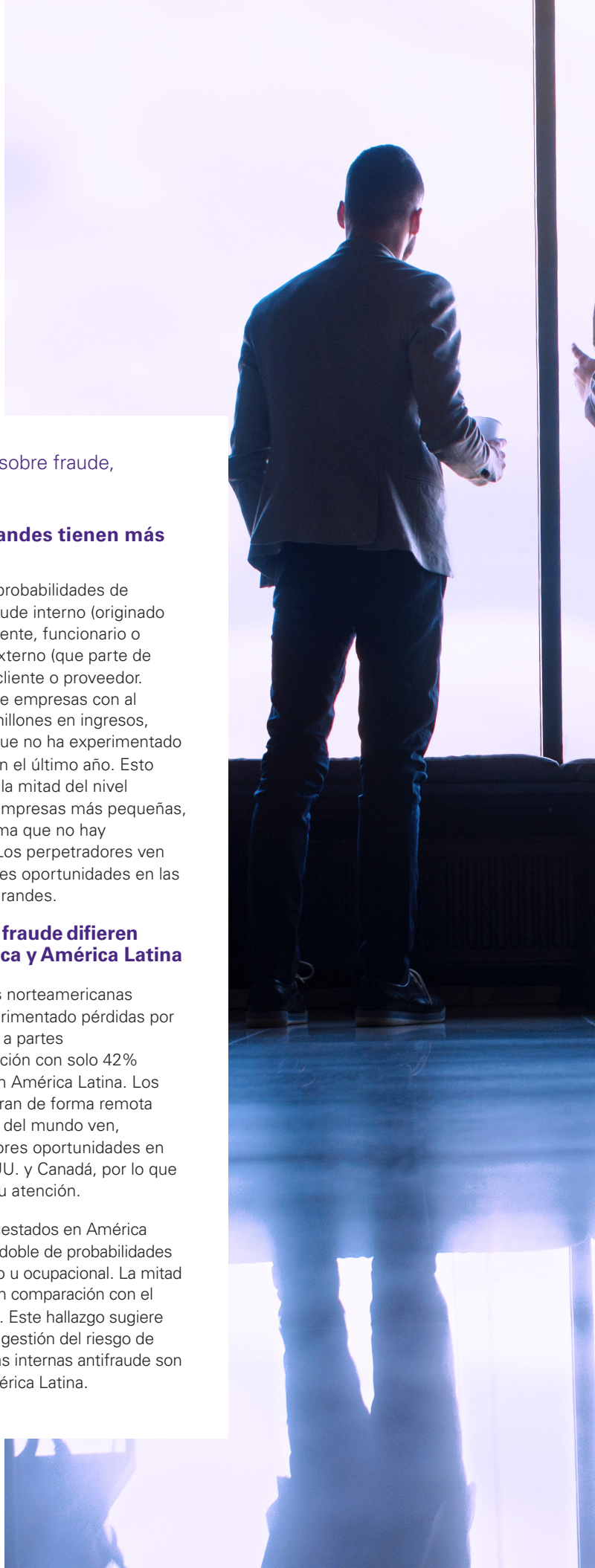
2022 KPMG Fraud Outlook

Enero 2022

KPMG.com

Contenido

Introducción



KPMG[1] se complace en presentar las perspectivas para 2022 sobre fraude, ciberataques y temas de cumplimiento en las Américas.

Encuestamos a más de 600 directivos de múltiples industrias para confirmar la evidencia anecdótica de los efectos de la pandemia con respecto a estas tres amenazas interconectadas. El estudio revela que el fraude, las preocupaciones por el cumplimiento y los ciberataques son comunes, más graves, y se espera que aumenten su frecuencia.

¿Las empresas de las Américas están logrando defenderse de esta triple amenaza? Nuestra investigación sugiere que muchas cuentan con defensas limitadas, y que el cambio al trabajo híbrido o remoto está provocando que los controles existentes sean menos efectivos.

La mayoría de las empresas en Norteamérica y América Latina informaron que han sufrido pérdidas por fraude, infracciones de cumplimiento o ciberataques

83% de las personas encuestadas afirman que su empresa ha padecido al menos un ciberataque en los últimos 12 meses, y 71% ha sufrido fraudes. Asimismo, más de la mitad afirma haber pagado multas por aspectos regulatorios o sufrido económicamente debido a riesgos de cumplimiento no mitigados.

Todo esto, sumado, representa costos significativos. La muestra reporta que las pérdidas por fraude o incumplimiento representan 1% de las ganancias en el último año.

Las empresas grandes tienen más riesgo de fraude

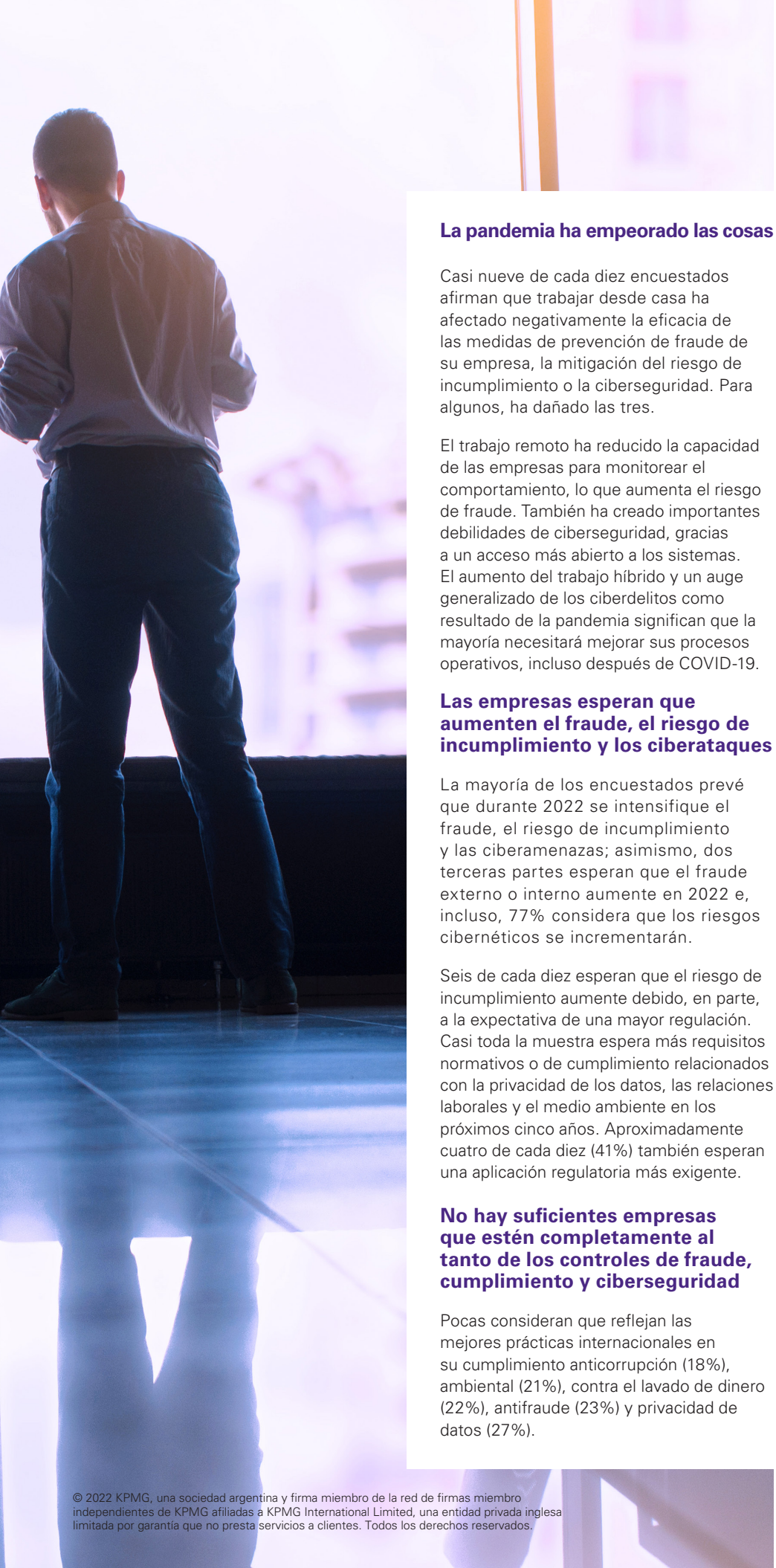
También tienen más probabilidades de sufrir pérdidas por fraude interno (originado por un empleado, gerente, funcionario o propietario o fraude externo (que parte de un tercero, como un cliente o proveedor. De los encuestados de empresas con al menos USD 10,000 millones en ingresos, sólo 15% considera que no ha experimentado pérdidas por fraude en el último año. Esto es aproximadamente la mitad del nivel observado entre las empresas más pequeñas, de las que 29% informa que no hay pérdidas por fraude. Los perpetradores ven claramente las mayores oportunidades en las organizaciones más grandes.

Las amenazas de fraude difieren entre Norteamérica y América Latina

76% de las empresas norteamericanas señalan que han experimentado pérdidas por fraude que involucran a partes externas, en comparación con solo 42% de los encuestados en América Latina. Los delincuentes que operan de forma remota desde cualquier parte del mundo ven, aparentemente, mayores oportunidades en las empresas de EE.UU. y Canadá, por lo que están centrando allí su atención.

Sin embargo, los encuestados en América Latina tienen más del doble de probabilidades de sufrir fraude interno u ocupacional. La mitad (49%) informa esto, en comparación con el 17% de Norteamérica. Este hallazgo sugiere que los programas de gestión del riesgo de fraude y otras defensas internas antifraude son menos sólidos en América Latina.

1 Cualquier referencia a KPMG en este informe se refiere a una colaboración entre las firmas miembro de KPMG en América Latina, EE.UU. y Canadá para producir nuestros conocimientos de investigación.



La pandemia ha empeorado las cosas

Casi nueve de cada diez encuestados afirman que trabajar desde casa ha afectado negativamente la eficacia de las medidas de prevención de fraude de su empresa, la mitigación del riesgo de incumplimiento o la ciberseguridad. Para algunos, ha dañado las tres.

El trabajo remoto ha reducido la capacidad de las empresas para monitorear el comportamiento, lo que aumenta el riesgo de fraude. También ha creado importantes debilidades de ciberseguridad, gracias a un acceso más abierto a los sistemas. El aumento del trabajo híbrido y un auge generalizado de los ciberdelitos como resultado de la pandemia significan que la mayoría necesitará mejorar sus procesos operativos, incluso después de COVID-19.

Las empresas esperan que aumenten el fraude, el riesgo de incumplimiento y los ciberataques

La mayoría de los encuestados prevé que durante 2022 se intensifique el fraude, el riesgo de incumplimiento y las ciberamenazas; asimismo, dos terceras partes esperan que el fraude externo o interno aumente en 2022 e, incluso, 77% considera que los riesgos cibernéticos se incrementarán.

Seis de cada diez esperan que el riesgo de incumplimiento aumente debido, en parte, a la expectativa de una mayor regulación. Casi toda la muestra espera más requisitos normativos o de cumplimiento relacionados con la privacidad de los datos, las relaciones laborales y el medio ambiente en los próximos cinco años. Aproximadamente cuatro de cada diez (41%) también esperan una aplicación regulatoria más exigente.

No hay suficientes empresas que estén completamente al tanto de los controles de fraude, cumplimiento y ciberseguridad

Pocas consideran que reflejan las mejores prácticas internacionales en su cumplimiento anticorrupción (18%), ambiental (21%), contra el lavado de dinero (22%), antifraude (23%) y privacidad de datos (27%).

Al observar específicamente cómo las empresas se desempeñan en una serie de medidas relacionadas con el control del fraude, el cumplimiento y la ciberseguridad, encontramos que sólo una pequeña proporción informa controles estrictos en al menos la mitad de las medidas relevantes (a la que nos referimos como el estándar "la mitad o más"). Sólo 24% se considera sólida en la mitad o más de las protecciones de ciberseguridad relevantes; 17%, en los controles para prevenir y detectar el fraude, y 13%, en abordar los riesgos de cumplimiento. Sólo 4% considera que sobresale en las tres áreas.

Las empresas tienen prioridades urgentes

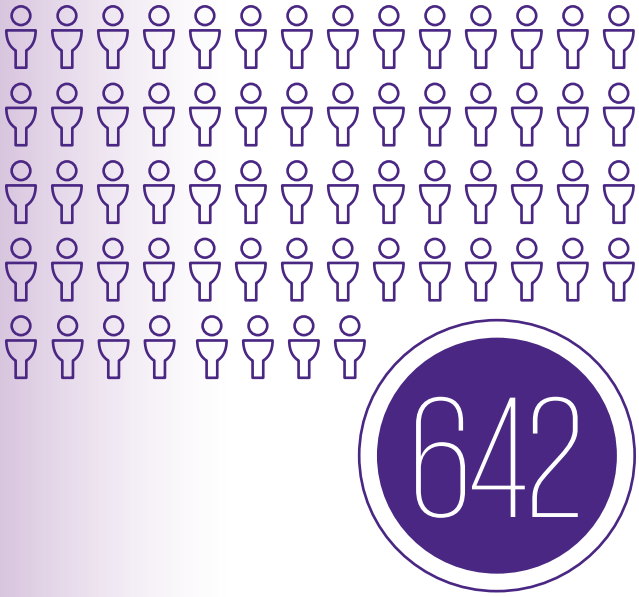
Fraude:
Nunca hay que descartar la posibilidad de que su origen sea interno (*an inside job*). En el último año, un revelador 31% reconoce que ha sufrido fraudes perpetrados por un colaborador

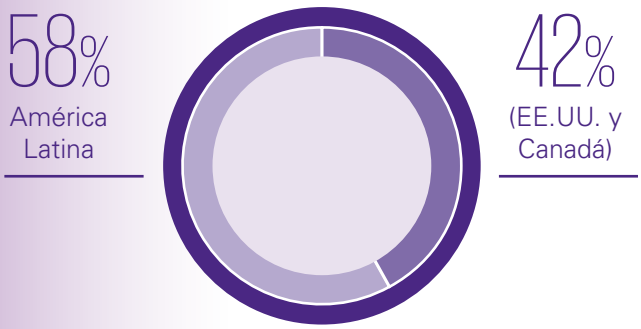
Cumplimiento:
Es ahora un tema reputacional. La mayoría afirma que las consideraciones de reputación hacen que el liderazgo de la empresa preste atención al cumplimiento en comparación con aquellos que afirman lo mismo sobre multas y la aplicación de la ley

Ciberseguridad:
Quienes sean lentos e inflexibles no ganarán la carrera de la ciberseguridad. Las personas participantes en el estudio afirman que se necesita alrededor de un mes, en promedio, para contener por completo un ciberataque, pero la mayoría parece estar satisfecha con su desempeño en esta área. Lo anterior indica que existe una falta de sentido de urgencia, potencialmente fatal

Acerca de la encuesta

Este estudio se basa en una encuesta a 642 personas en puestos directivos:





Estas personas integran, de manera casi uniforme, las siguientes 7 industrias:

Manufactura industrial

Productos de consumo y *retail*

Energía y recursos naturales

Servicios financiero

Seguros

Ciencias de la vida e industria farmacéutica

Telecomunicaciones, tecnología, medios y entretenimiento

La muestra está compuesta predominantemente por líderes en posiciones de Alta Dirección: **más de la mitad pertenecen al Consejo de Administración, son nivel C o jefes de departamento.**

Acerca de la encuesta (Continuación)

Las empresas son de diversos tamaños:

tiene ingresos anuales menores a **USD 1,000 millones**

tiene ingresos anuales de entre **USD 1,000 millones y USD 10,000 millones**

tiene ingresos anuales mayores a **USD 10,000 millones**

También se entrevistó a seis líderes corporativos y especialistas en toda la región:

José Calderón
Chief Global Auditing Office, Grupo Bimbo

Larissa Galimberti
Partner, Pinheiro Neto Advogados

Carlos García Jiménez
Regional Director of Ethics and Compliance LATAM, Uber

Ariel Nowersztern
Cybersecurity Specialist, Inter-American Development Bank

Beth Rose
Chief Compliance, Ethics and Integrity Office, Ford Motor Company

Pascal Saint-Amans
Director, Center for Tax Policy and Administration, OECD

Les agradecemos por compartir sus perspectivas.

Una defensa unida contra una triple amenaza

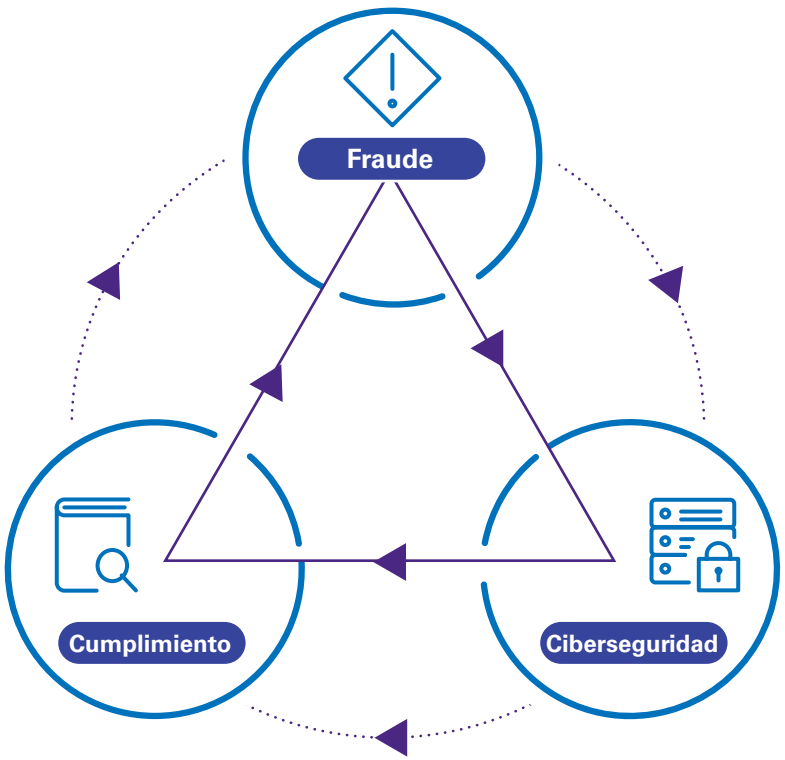
El fraude, los riesgos de incumplimiento y los ciberataques se generalizan, representando peligros cada vez mayores para las empresas en Norteamérica y América Latina.

Estas amenazas están entrelazadas. Consideremos, por ejemplo, el caso de un empleado que roba datos de un cliente de la empresa mientras trabaja desde casa; esto genera las tres amenazas simultáneamente, de modo que las empresas deben abordarlas como una sola.

Las compañías necesitan mitigar lo que en KPMG llamamos el "ciclo de la amenaza", que comprende: fraude, riesgo de incumplimiento y amenazas a la ciberseguridad.

Defenderse contra estas amenazas requiere un esfuerzo colectivo e interconectado, en el cual las empresas consideren el impacto que crean en su conjunto, en vez de mirar, de manera aislada, los riesgos que implican.

El ciclo de la amenaza según KPMG



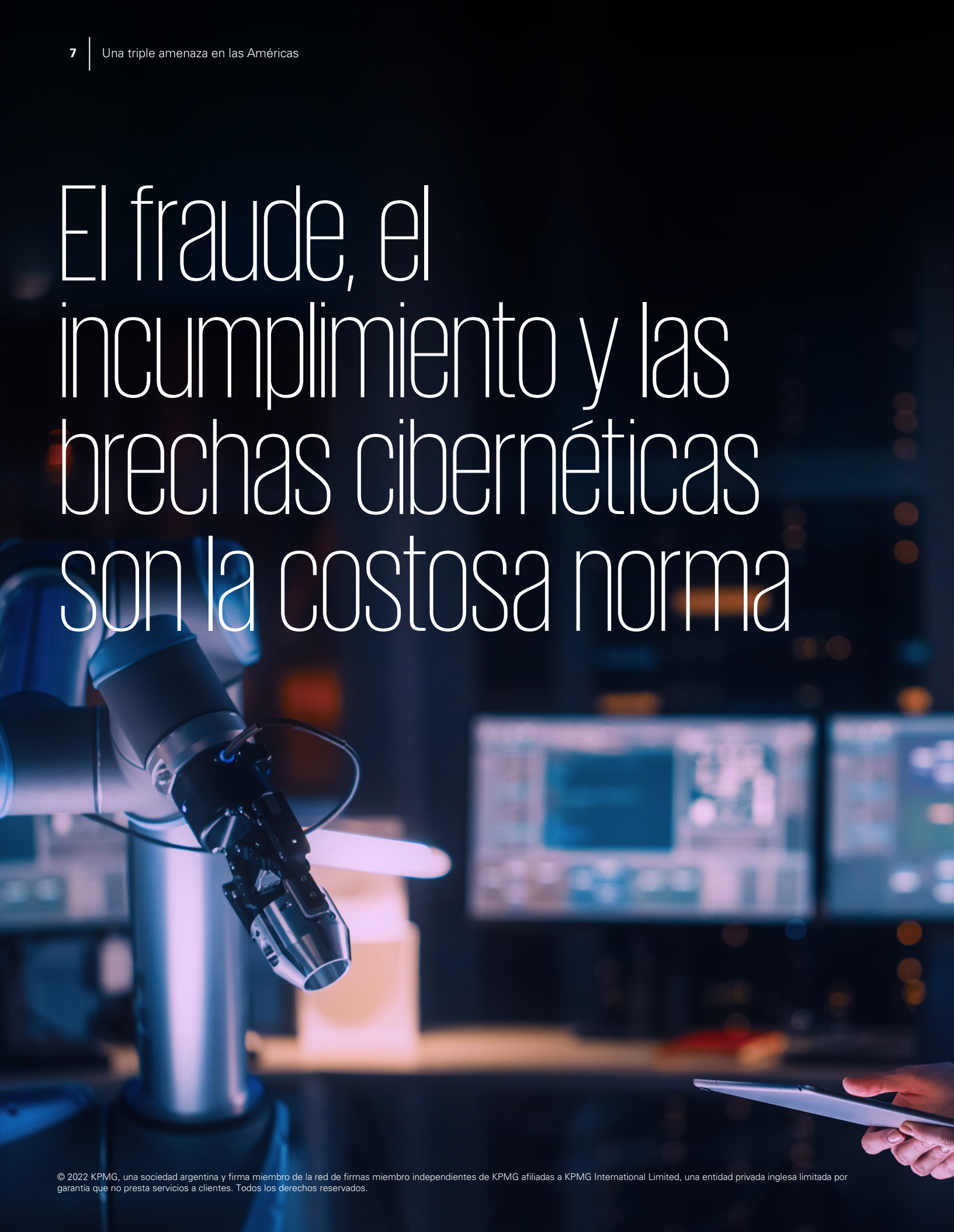
Ariel Nowersztern, Cybersecurity Specialist, Inter-American Development Bank (BID), afirma que algunas empresas ya están desarrollando defensas holísticas contra estos riesgos. "Puedes utilizar cualquiera de los métodos de ciberseguridad, control interno y auditoría para mejorar la eficacia de los demás", explica.

Algunas empresas han combinado el monitoreo de activos físicos y digitales con controles antifraude y otros controles internos. Una alerta en un área podría indicar que algo anda mal en otra.

Para saber si las empresas están preparadas para responder a este ciclo de amenazas y cuánto trabajo deben hacer si aún no están listas, encuestamos a la Alta Dirección de diversas organizaciones de Norteamérica y América Latina. Este informe analiza su perspectiva ante la pregunta: ¿están preparadas las empresas de las Américas?

> "Puede utilizar cualquiera de los métodos de ciberseguridad, control interno y auditoría para mejorar la eficacia de los demás"
>
> **Ariel Nowersztern**
> Especialista en ciberseguridad de Inter-American Development Bank (BID)

El fraude, el incumplimiento y las brechas cibernéticas son la costosa norma



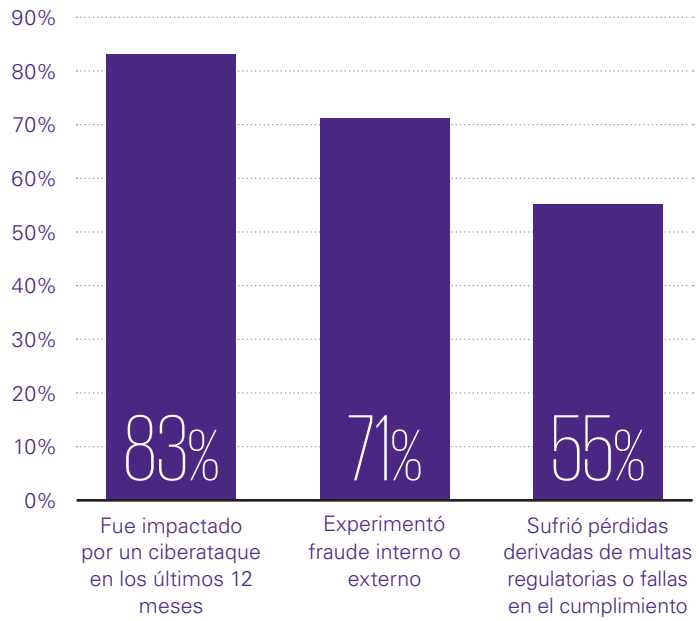
“Ahora se trata de cuándo sucederá un ciberataque, no de si ocurrirá”, afirma Larissa Galimberti, Partner especializada en temas de tecnología del bufete de abogados brasileño Pinheiro Neto Advogados. Los encuestados coinciden en que, para las empresas en las Américas, los intentos de fraude y las brechas de cumplimiento son inevitables.

De los riesgos que examinamos, los encuestados indican que es más probable que sus empresas hayan experimentado ciberataques. En general, 83% afirma que su empresa ha sufrido al menos un ciberataque en los últimos 12 meses. La encuesta pidió señalar sólo los incidentes con un impacto notable en el negocio, por lo que es probable que el número total de ciberataques sea mayor al informado.

El fraude también se cita con preocupante frecuencia: hasta 71% informa que su empresa descubrió fraudes durante los últimos 12 meses; esto se eleva a 85% en las empresas con más de USD 10,000 millones de ingresos anuales. Mientras tanto, 55% también reconoce que su negocio ha tenido que pagar multas por temas regulatorios o ha sufrido económicamente debido a infracciones al cumplimiento en el último año.

Los casos no descubiertos de fraude e incumplimiento sugieren que es probable que estos números no sean representativos y que el problema subyacente sea aún mayor.

La realidad de la amenaza triple



La muestra encuestada reporta que las empresas tienen una pérdida combinada promedio por fraude, temas de cumplimiento y multas por aspectos regulatorios de 1% de sus ganancias. Además, 58% reconoce haber sufrido una pérdida económica directa a causa de un ciberataque. Mientras tanto, 20% reporta que la compañía sufrió daños a su reputación, y 32%, que tuvo que lidiar con una investigación de cumplimiento.

Estos incidentes pueden representar una amenaza a la permanencia, advierte Nowersztern, especialmente para las empresas más pequeñas. La pérdida sustancial de capital, una reputación gravemente dañada o, incluso, la exposición de información operativa clave (como listas de clientes, pueden provocar el colapso de una organización.

Los costos en estas áreas crecen con el tamaño de la empresa. Los encuestados de aquellas empresas con ingresos anuales superiores a USD 10,000 millones afirman que, en promedio, su compañía perdió 0.7% de las ganancias netas por fraude el año previo y pagaron 0.8% de las ganancias netas como multas por incumplimiento, dando un total de 1.5%.

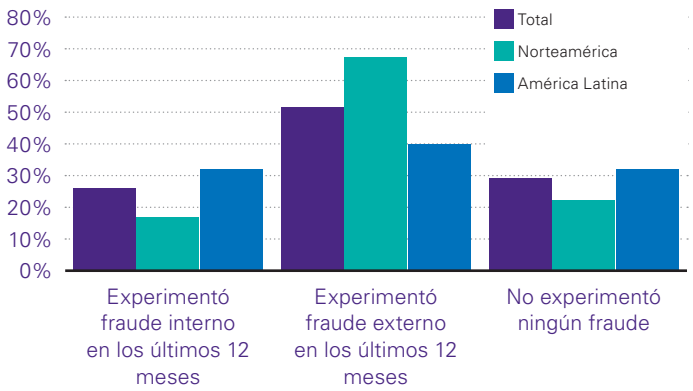
Beth Rose, Chief Compliance, Ethics and Integrity Officer, Ford Motor Company, enfatiza que estas cifras no son la única razón por la que el cumplimiento, la prevención del fraude y la ciberseguridad son importantes para las corporaciones. En las buenas empresas, la reputación y la probidad son consideraciones cruciales; sin embargo, los costos de la magnitud citada, también son relevantes para las organizaciones y sus grupos de interés. "Los directivos están naturalmente inclinados a mirar el impacto económico", reconoce Rose.

Carlos García Jiménez, Regional Director of Ethics and Compliance LATAM, Uber, está de acuerdo con lo anterior, y señala que la protección efectiva contra dichos riesgos "cuesta una fracción" de las pérdidas promedio de todas las empresas comparadas.

Diferencias regionales de fraude y por qué es importante el tamaño de la empresa

A primera vista, tanto en Norteamérica como en América Latina se informa de incidentes de fraude distintos, como se aprecia en la siguiente gráfica.

Comparando el fraude en Norteamérica y América Latina

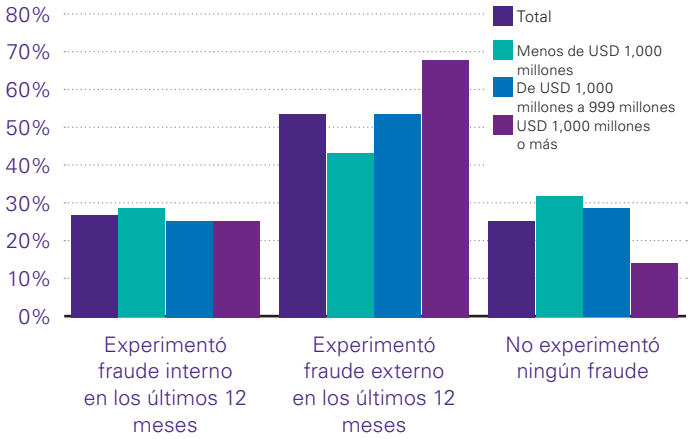


Vale la pena hacer dos observaciones. Primero, la muestra indica que el fraude es un problema más extendido para las empresas en Norteamérica. En segundo lugar, el entorno de riesgo difiere entre regiones. Las empresas en América Latina tienen casi el doble de probabilidades de que colaboradores con información privilegiada estén involucrados en el fraude. En Norteamérica, en cambio, el fraude externo es un problema mucho mayor.

1.5%: el porcentaje de ganancias que las grandes empresas están perdiendo debido al fraude y al incumplimiento

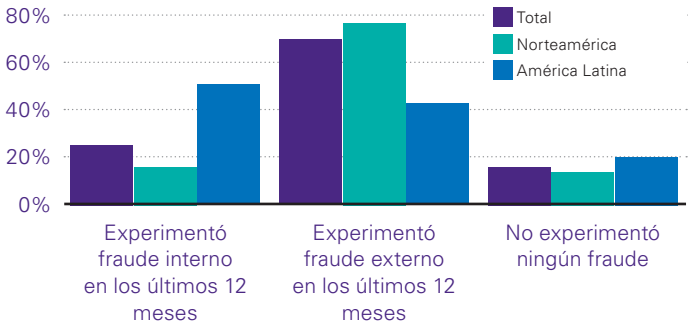
Las cifras probablemente se vean afectadas por la fuerte variación en el tamaño medio de las empresas entre las dos regiones. La mayoría de las empresas encuestadas en Norteamérica son considerablemente más grandes, con ingresos anuales medios de USD 2,900 millones, en comparación con los USD 846 millones de las organizaciones en América Latina. Nuestra encuesta también muestra que las empresas más grandes y prósperas suelen ser blanco de fraudes externos.

Comparando el fraude por tamaño de empresa



Pero ¿cuántas de las aparentes diferencias regionales se deben al tamaño de la empresa? Una respuesta proviene de comparar sólo las empresas más grandes, aquellas con ingresos de USD 10,000 millones o más, en cada región de las Américas.

Comparando el fraude: compañías con al menos USD 10,000 de ingresos anuales



Al comparar la muestra de grandes empresas por región, las cifras de los afectados por algún fraude convergen. La brecha entre la proporción de todas las empresas en Norteamérica que experimentan algún fraude (77% y la misma cantidad en América Latina (67% es de diez puntos porcentuales. Sin embargo, entre las empresas más grandes, 86% en Norteamérica informa de algún fraude en los últimos 12 meses, y 80% lo hace en América Latina, una diferencia que resulta menor.

Sin embargo, los resultados para diferentes tipos de fraude divergen notablemente. Entre las grandes empresas en América Latina, 49% reconoce que al menos un fraude interno había ocurrido en el último año: casi tres veces la tasa de Norteamérica. Esto sugiere que, si bien las empresas en Norteamérica están lejos de ser inmunes al fraude interno, las empresas en América Latina necesitan priorizar la implementación de controles internos para abordar el riesgo de fraude interno.

¿Qué debe hacerse con el porcentaje mucho mayor de empresas en Norteamérica que han experimentado fraude externo (76%, en comparación con el 42% de América Latina? Una explicación probable radica en la experiencia divergente del cibercrimen. De la muestra de grandes empresas en América Latina, sólo 7% reporta un ciberataque en el último año. En Norteamérica, 43% experimentó uno en ese mismo lapso.

Además de tener mayores ingresos, Nowersztern sugiere que los blancos de ataque en Norteamérica están más digitalizados y, por lo tanto, tienen una mayor exposición. Alternativamente, pueden ser mejores para detectar cuándo ocurre un ciberataque, por lo que las tasas reales de intento de incursión en las empresas de todo el continente pueden estar más cerca de lo que se refleja en las respuestas. Está claro que las empresas en Norteamérica necesitan mejores ciberdefensas, pero las empresas en América Latina no pueden ser autocomplacientes; a medida que crezcan, se convertirán en objetivos más atractivos para los ciberataques.

Instantánea de datos I: una bandada de estafadores

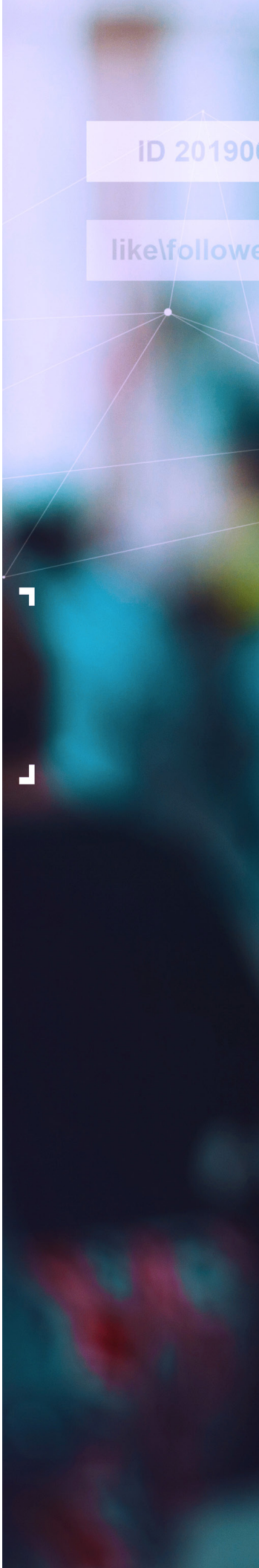
¿Cuál de las siguientes clases de individuo se sabe que estuvo involucrada en un fraude o mal comportamiento (sólo o en colusión) en su compañía durante los últimos 12 meses?

Las empresas son vulnerables a una amplia gama de estafadores. José Calderón, Chief Global Auditing Officer, Grupo Bimbo, explica que su empresa ha implementado un marco global para reducir una variedad de riesgos de fraude. "Todo lo que puede afectar los procesos, desde el abastecimiento de materia prima de varios proveedores, pasando por la producción, hasta las ventas y la ejecución", sugiere, pueden originar un riesgo de fraude. "Entonces, también existen desafíos sobre cumplimiento y fraude con asociados internos y externos, regulaciones ambientales y laborales, privacidad de datos; el riesgo es muy extenso".

Según la encuesta, el tipo de delincuente que se infiltra con más frecuencia en las empresas o, al menos, se descubre más frecuentemente, es el ladrón externo, a menudo habilitado digitalmente. Muy cerca se encuentran socios de negocio y proveedores. En aquellos países donde las operaciones locales de la empresa tienen pocos controles establecidos y cuenta con un gran número de terceros proveedores, el potencial de fraude o colusión resulta proporcionalmente grande.

También existe la amenaza interna: 31% de la muestra informa que, en el último año, se cometió fraude interno en su empresa (por parte de un empleado, gerente, funcionario o propietario).

Los culpables también varían según la región. En Norteamérica, 43% cita casos de fraude perpetrados por una organización delictiva externa (como un grupo de piratas informáticos), y en América Latina este porcentaje es de sólo 14%. Por el contrario, en América Latina 36% reconoce que su empresa experimentó un fraude interno, cifra que se reduce a 23% en las empresas de Norteamérica.



¿Cómo cambió el panorama por la pandemia?

COVID-19 y los confinamientos resultantes han complicado el entorno de amenazas.

En todas las áreas, el entorno de riesgo ha empeorado, mientras que el aumento del trabajo remoto ha mermado las defensas existentes. En general, 86% afirma que el trabajo a distancia ha afectado negativamente al menos un elemento de los programas de prevención de fraude, cumplimiento y ciberseguridad en la empresa.

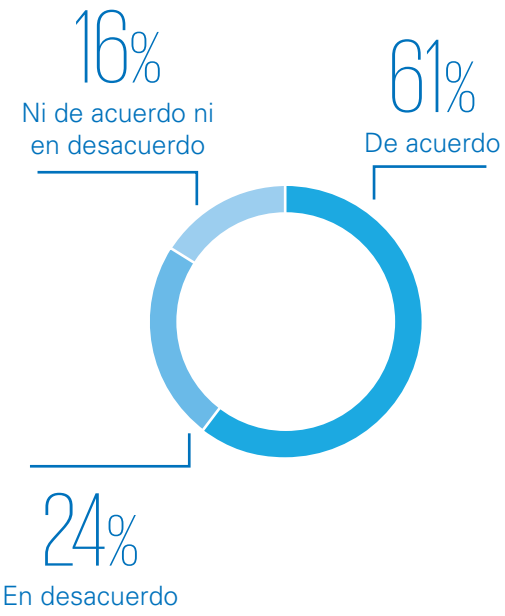
86% afirma que el trabajo a distancia ha afectado negativamente al menos un elemento de los programas de prevención de fraude, cumplimiento o ciberseguridad de su empresa

Prevención del fraude

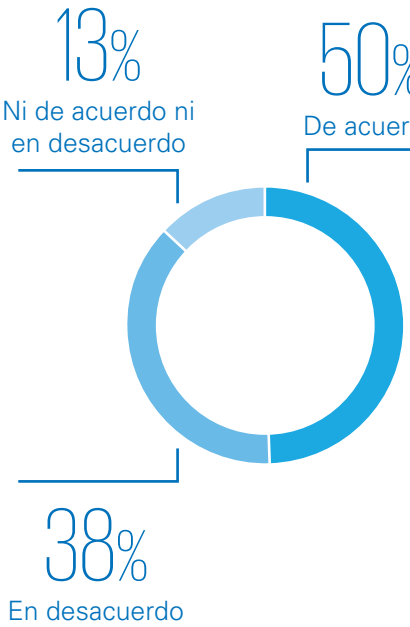
Las oportunidades de fraude dentro de una empresa son producto de sus operaciones. Por ejemplo, la necesidad de obtener materias primas y repuestos de manera expedita genera riesgos sustanciales, comenta José Calderón, de Bimbo.

Esto se debe a que es más probable que las empresas eludan los controles existentes (como la diligencia debida sobre terceros para obtener acceso a esos materiales lo más pronto posible. Este fue un riesgo particular para muchas empresas, tanto en el punto más bajo de la pandemia como en medio de los problemas de la cadena de suministro en gran parte del mundo, a fines de 2021.

El cambio al trabajo a distancia ha incrementado los riesgos de fraude, debido a una capacidad reducida para monitorear y controlar el comportamiento fraudulento



Trabajar desde casa ha impactado negativamente nuestra capacidad para responder apropiadamente al fraude en nuestro negocio



Mientras tanto, el rápido aumento del trabajo remoto también representa desafíos para la prevención del fraude, especialmente para la supervisión y la investigación. En este sentido, 61% indica un mayor riesgo de fraude debido a una menor capacidad para monitorear el comportamiento de los colaboradores.

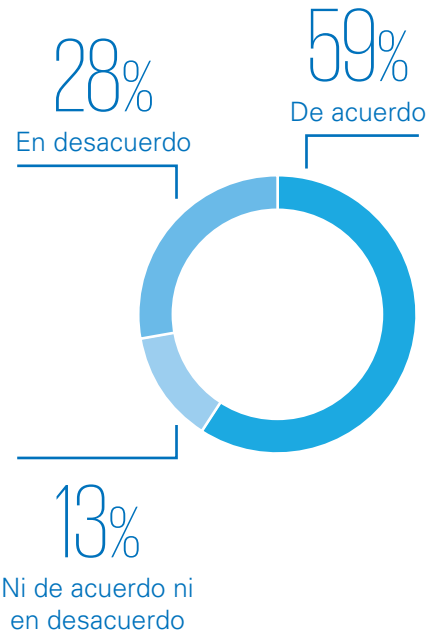
Pero esto no está relacionado únicamente con los colaboradores operativos; si bien 28% informa que el trabajo remoto ha impedido los controles de gestión y la supervisión, el problema va más allá de que los empleados tengan un lugar de trabajo nuevo y remoto. Por ejemplo, como afirma García Jiménez, muchos empleados son *millennials* que comparten departamento con personas ajenas a la empresa. Debido a esto, asegurarse de que personas ajenas no tengan el acceso a los sistemas de la compañía se convirtió en un desafío mayor.

Del mismo modo, la mitad de la muestra señala que trabajar desde casa ha afectado negativamente la capacidad de la empresa para responder al fraude. García Jiménez señala que incluso los controles básicos de fraude han tenido que cambiar.

Fuera de un entorno normal de oficina, los investigadores ya no tienen el mismo nivel de control físico de una situación. "Es un gran desafío recopilar información o recuperar archivos y correos electrónicos. Incluso realizar una entrevista [es más difícil]. Desde una perspectiva logística, es necesario desarrollar arreglos diferentes a los del pasado, [no sólo] reservar un espacio". Algunos empleados pueden, incluso, estar trabajando de forma remota desde otro estado o país.

Es poco probable que estos desafíos desaparezcan, y se espera que el trabajo híbrido sea cada vez más común. La mayoría de las empresas en las Américas siguen sin estar preparadas para responder a estos riesgos: 59% está de acuerdo en que "los controles antifraude establecidos antes de la pandemia no se han actualizado de manera efectiva para reflejar la nueva realidad laboral".

Los controles antifraude establecidos antes de la pandemia no se han actualizado de manera efectiva para reflejar la nueva realidad laboral



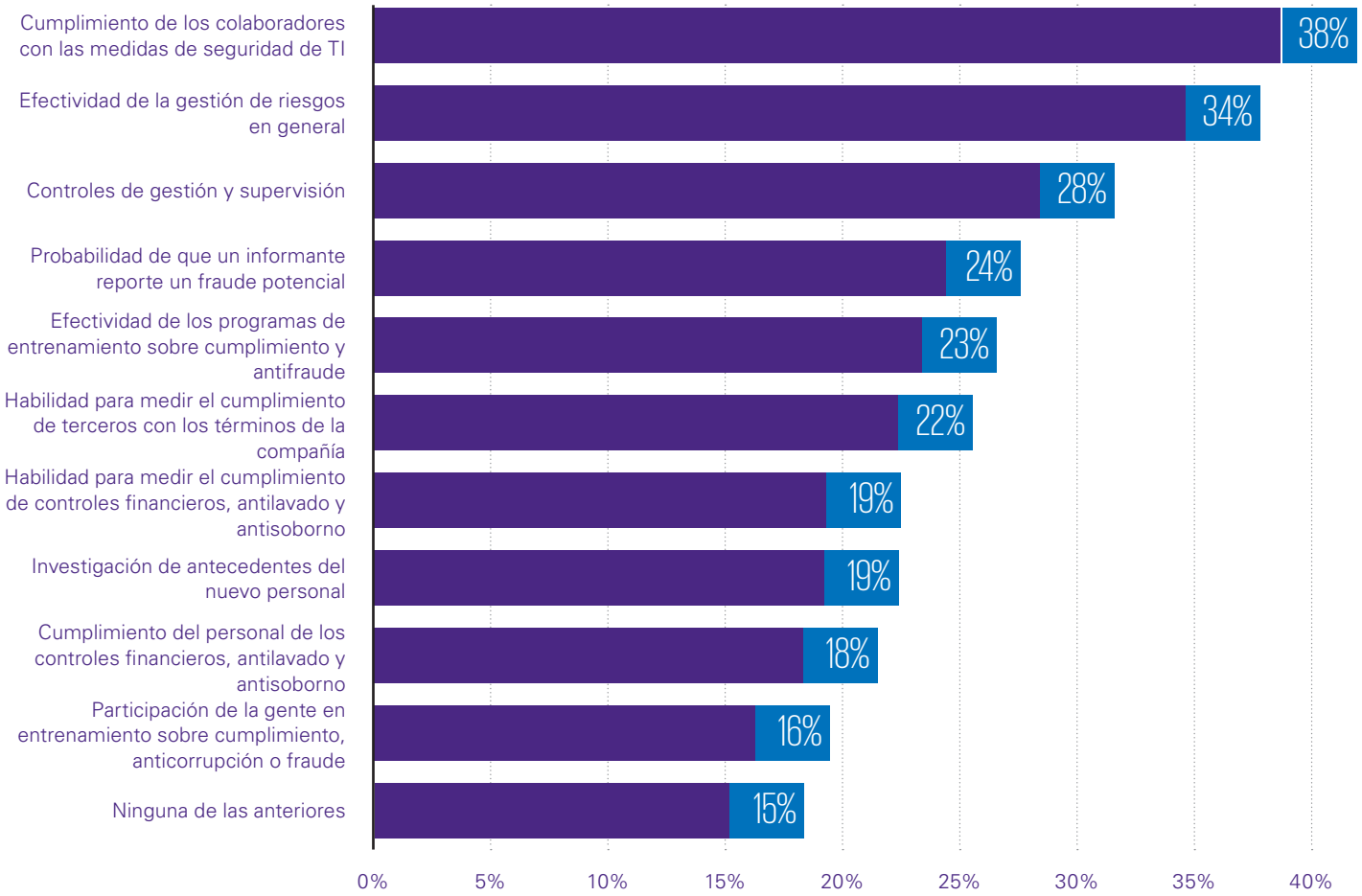
59% está de acuerdo en que los controles antifraude establecidos antes de la pandemia no se han actualizado de manera efectiva para reflejar la nueva realidad laboral

Cumplimiento

Hasta 77% afirma que su empresa tuvo que desarrollar nuevas estrategias durante la pandemia para mantenerse al día con las cambiantes demandas de cumplimiento. En algunos casos, esto reflejó los nuevos desafíos de la situación.

Beth Rose, de Ford, recuerda que "COVID-19 requirió un gran cambio de cada departamento de cumplimiento". La pregunta inicial fue "¿Cómo se cumple con la salud y la seguridad?". De manera similar, cuando Ford comenzó a fabricar ventiladores y respiradores por primera vez, tuvo que comprender e implementar los requisitos de cumplimiento relacionados con estos productos.

¿Qué aspectos se han visto impactados negativamente por el aumento de colaboradores trabajando desde casa en el último año?



Las consideraciones de trabajo remoto también han jugado un papel importante en el cumplimiento. García Jiménez sugiere que la capacitación para el cumplimiento tuvo el mayor impacto, con cursos presenciales que luego fueron en línea. Se trata de más que un cambio del medio de interacción que, para muchas empresas, requirió una revisión sustancial de los materiales de capacitación y el desarrollo de diferentes habilidades de comunicación de quienes capacitan y los que aprenden. Para muchos, el tiempo requerido fue causa de una brecha prolongada en el entrenamiento.

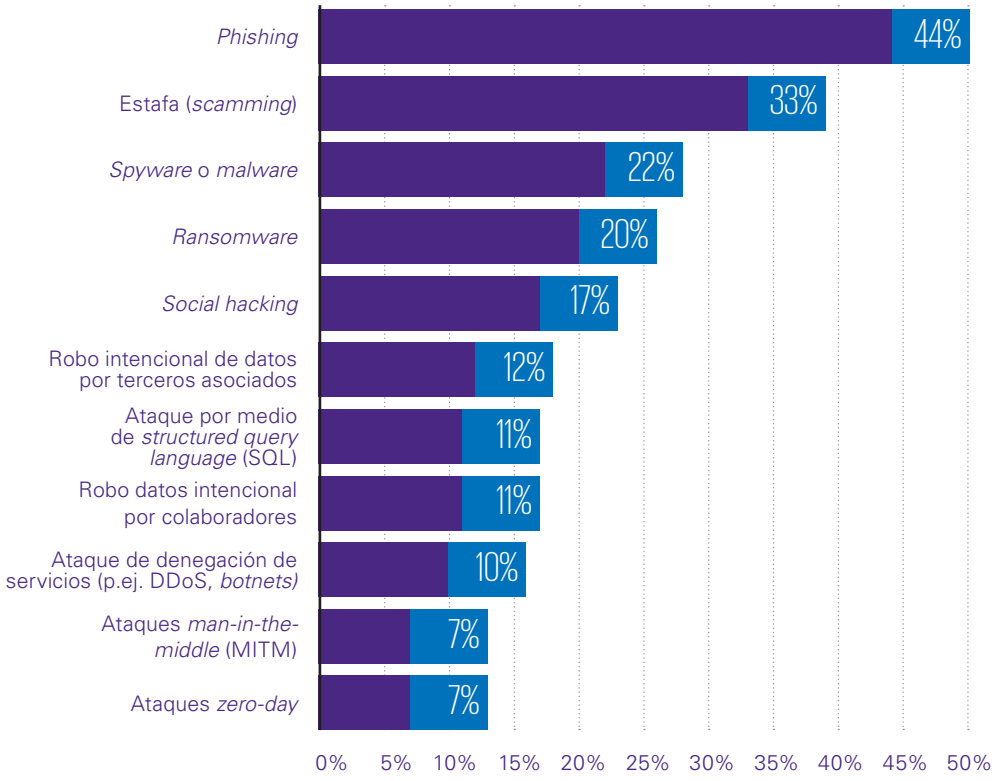
El aumento del trabajo a distancia también exigió un cambio cultural sustancial. "Parte del cumplimiento es ver lo que está sucediendo para tener una idea de dónde podría haber algún riesgo", señala Rose. "Cuando nos volvimos virtuales, eso se convirtió en un problema". Muchos encuestados están de acuerdo: 19% señala que el trabajo remoto dificulta la medición del cumplimiento de los controles financieros contra el lavado de dinero y el soborno.

La adaptación al nuevo entorno de cumplimiento sigue siendo un proceso en desarrollo. Beth Rose indica que Ford planea continuar con su actual modelo de trabajo híbrido. Averiguar las implicaciones para el cumplimiento es "la pregunta del millón de dólares. Tenemos que pensar diferente" en formación, sensibilización, equipos y evaluación de riesgos, afirma. Las diferentes industrias tendrán necesidades distintas.

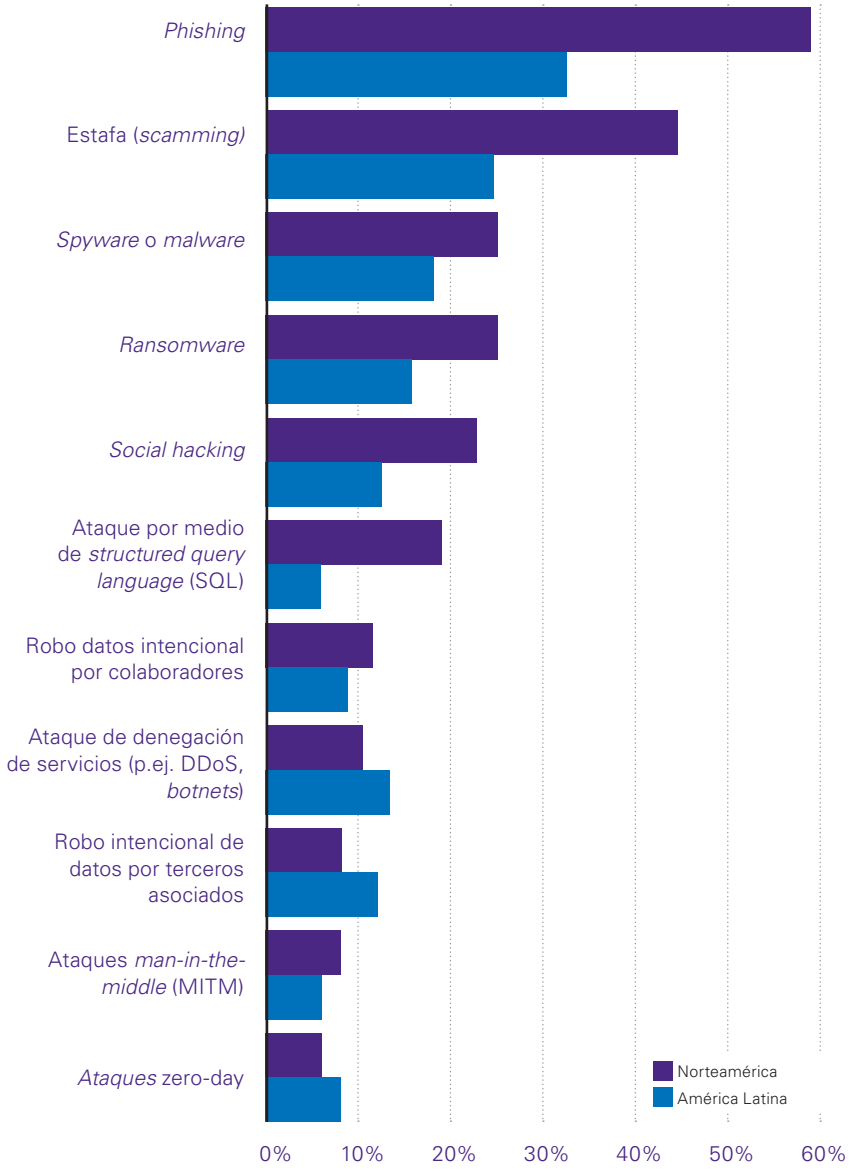
Ciberseguridad

El cibercrimen aumentó en volumen durante la pandemia, y no ha disminuido. Como muestra la gráfica, las empresas encuestadas reportan aumentos en la frecuencia de varios tipos de ataques, como *phishing* (citado por 44%), estafa (33%), *malware* (22%) y *ransomware* (20%), que representan crecientes desafíos para muchas. En general, 79% vio un crecimiento en al menos uno de los tipos de ataque cubiertos en la encuesta.

¿Cuáles de los siguiente ciberataques han incrementado en su empresa en los últimos 12 meses (si fuera el caso)?



Comparando por región, ¿en cuál ha visto un incremento en el último año?



Incluso los incidentes individuales pueden tener un gran impacto. Por ejemplo, un ataque de *ransomware* en un oleoducto en mayo de 2021 provocó escasez de petróleo en varios estados del sur de EE.UU. Como otro ejemplo con un efecto sustancial, Galimberti cita un importante robo de datos que tuvo lugar en Brasil a principios de 2021: "Se colocaron archivos de 220 millones de brasileños en la *dark* web con todo tipo de información", afirma.

Nowersztern señala que varias tendencias previas a la pandemia, y que fueron aceleradas por esta, ayudaron a impulsar el crecimiento de la actividad delictiva. Por ejemplo, los mensajes de phishing abordaron temas de actualidad de COVID-19 para atraer a consumidores ansiosos. Además, a medida que las empresas y la sociedad se han vuelto más dependientes de los activos y equipos digitales, advierte, "ahora somos, incluso, más vulnerables de lo que solíamos ser. Los criminales han tomado nota".

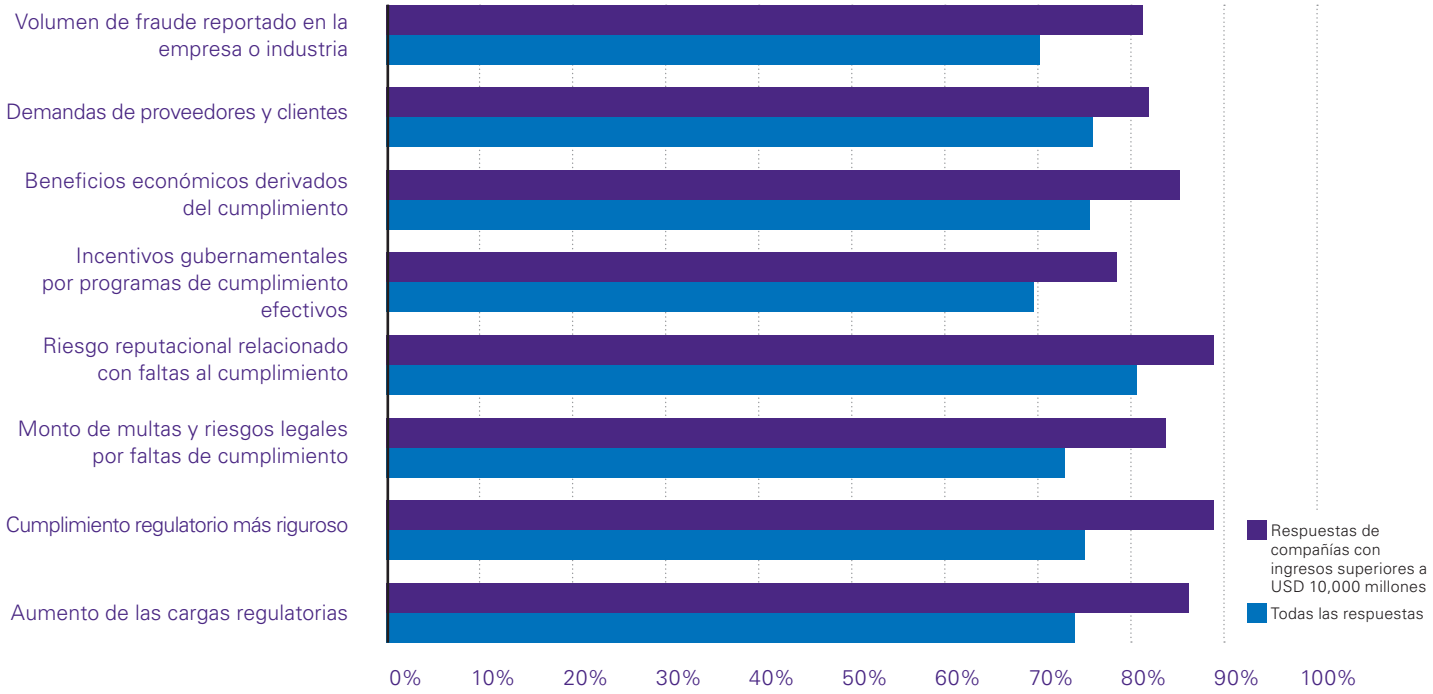
Casi toda la muestra señala que su empresa había tomado medidas para abordar los riesgos de ciberseguridad, incluida la implementación de autenticación de dos factores (55%), mejoras en la seguridad de la red (54%) y una mejor capacitación (47%). La inversión resultante, necesaria para hacer frente a estos desafíos, podría ser sustancial. Calderón informa que, en Grupo Bimbo, "el Consejo aumentó el presupuesto de ciberseguridad más de cinco veces. Y podría aumentar más". Este incremento fue necesario a pesar de que menos de uno de cada cinco empleados de Grupo Bimbo trabaja desde casa.

69% reconoce que el trabajo a distancia ha sido un gran desafío de ciberseguridad para sus negocios

COVID-19 y el cambio relacionado con el trabajo a distancia han dificultado que las empresas aborden su ciberseguridad: 67% mantiene la preocupación por los riesgos cibernéticos de un entorno de trabajo híbrido. El fin de la pandemia, o al menos de los confinamientos, pueden vislumbrarlo algunos, pero los patrones de trabajo permanentemente alterados en las Américas implican que los esfuerzos en todos los aspectos del ciclo de amenazas requieren atención urgente.

Instantánea de datos II: el cumplimiento es una preocupación de todo el negocio

¿En qué medida los siguiente aspectos incrementan el tiempo y atención que el liderazgo de la empresa dedica a cuestiones de cumplimiento? (La gráfica muestra la proporción de encuestados que seleccionaron la opción 4 o 5 de una escala de 1 a 5, en la que 1 es "nada ", 3 es "un poco" y 5 es "mucho").



El cumplimiento ya no es, si alguna vez lo fue, simplemente una cuestión de mantenerse en el lado correcto de la ley. Como muestra la gráfica, más de 70% (y más de 80% de quienes trabajan en grandes empresas) indica que la aplicación rigurosa, el aumento de las cargas regulatorias y las posibles sanciones aumentan el tiempo y la atención que sus líderes corporativos prestan a los temas de cumplimiento.

Sin embargo, es muy probable que las demandas de los grupos de interés, los beneficios económicos y la reputación centren la atención del liderazgo de las empresas en el cumplimiento: 64% señala que los proveedores y clientes exigen cada vez más pruebas de cumplimiento de las regulaciones de privacidad de datos, y 52% afirma lo mismo sobre la corrupción y legislación sobre lavado de dinero.

Beth Rose, de Ford, no se sorprende: "Con la evolución de las redes sociales y la proliferación de personas que opinan sobre la reputación y la marca, hay que preocuparse por lograr el cumplimiento correcto". También son imperativos la aplicación estricta de las regulaciones y la importancia de evitar vincularse inadvertidamente mediante asociaciones y fusiones con terceros que no satisfagan patrones de cumplimiento.

Este conjunto más amplio de consideraciones incrementa el papel de la función de cumplimiento. García Jiménez comenta que, si bien el cumplimiento todavía consiste en mitigar el riesgo, ahora también se trata de "construir una narrativa, tanto interna como externamente". Parte del trabajo es mostrar a los reguladores, a otros grupos de interés y a la sociedad en general los beneficios económicos, sociales y ambientales que la empresa brinda a la comunidad.

De esta amplia narrativa construida, se desprenden otros beneficios para las empresas. En particular, un buen cumplimiento ayuda a comunicar la confiabilidad de una empresa a otros grupos de interés, ya sean reguladores, inversionistas, socios o clientes.

Los niveles de amenaza están aumentando

Los desafíos de trabajar de forma remota son sólo parte de un patrón más amplio de mayores dificultades relacionadas con el fraude, el cumplimiento y la ciberseguridad: 69% espera un aumento en el riesgo ya sea de fraude externo o interno durante los siguientes 12 meses, y 29% proyecta un incremento en el riesgo de ambos.

Las preocupaciones sobre el aumento de los ciberdelitos son generalizadas: 77% considera que el riesgo de ciberseguridad aumentará en los próximos 12 meses; sólo 7% prevé una disminución. Larissa Galimberti coincide al señalar que "las empresas se enfrentan a cada vez más piratas informáticos, *ransomware*, *phishing* y otros ataques".

El aumento de casos de fraude y ciberataques no siempre está relacionado. José Calderón señala que cualquier presión sobre los modelos operativos puede generar un aumento en el riesgo de fraude. En la industria de alimentos y bebidas, por ejemplo, el interés de los consumidores en productos más saludables a precios más bajos está reconfigurando la demanda. Un cambio hacia el uso de proveedores de menor costo para satisfacer esta nueva demanda requiere la debida diligencia relacionada con la forma en que estos operan, incluidas consideraciones tales como la forma en que se negocian los contratos y se aseguran de no mantener bajos los precios mediante el uso de procesos altamente contaminantes.

Sin embargo, el fraude y la ciberseguridad se superponen en un grado cada vez mayor. Los tipos de ciberataques para los que la mayor parte de la muestra ve aumentos en el último año incluyen *phishing* (44%, estafa (33%, software espía (22% y *ransomware* (20%.

69% espera un aumento en el riesgo de fraude externo o interno durante el próximo año

Las tendencias comerciales actuales aumentan inadvertidamente esta convergencia de fraude y riesgo cibernético al brindarles a los estafadores una nueva oportunidad. José Calderón señala, por ejemplo, que "la digitalización de procesos, ir a la nube [y] usar más dispositivos móviles" conlleva riesgos. Beth Rose agrega que "con todos a distancia y en computadoras, los criminales han encontrado formas más creativas de operar". Agrega que tales esfuerzos no están todos en línea. Los datos la respaldan: 17% señala un aumento en la piratería social, mediante la cual los ciberdelincuentes utilizan la ingeniería social y la manipulación de los comportamientos humanos para obtener acceso a los sistemas.

62%

Espera nuevas regulaciones sobre privacidad de datos en los próximos cinco años

47%

Espera nuevas regulaciones en materia ambiental en los próximos cinco años

46%

Espera nuevas regulaciones laborales en los próximos cinco años

41%

Espera una aplicación más estricta de las regulaciones existentes en los próximos cinco años

También es probable que el riesgo de incumplimiento general crezca el próximo año, según 60% de la muestra; sólo 17% espera una disminución en el riesgo de cumplimiento. Este desafío, como explica Beth Rose, de Ford, es multifacético e incluye más requisitos de cumplimiento en campos con una importante regulación existente; la probable introducción de reglas en nuevas áreas, y una aplicación más activa por parte de los funcionarios encargados del cumplimiento.

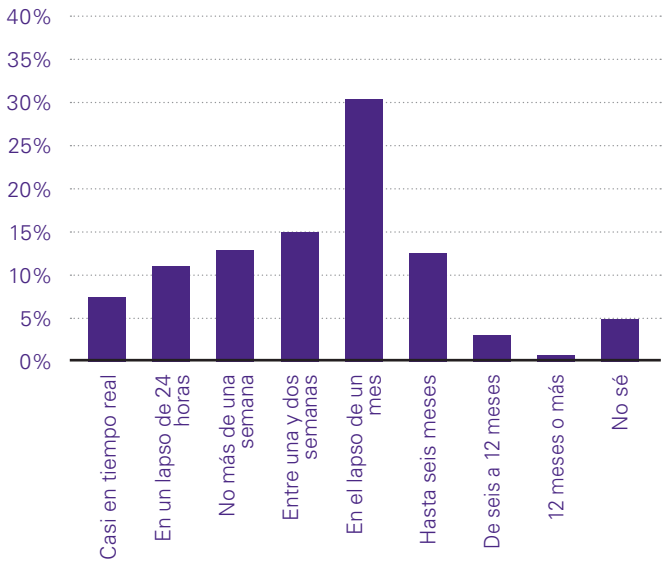
Como muestran los resultados, una cantidad sustancial de encuestados espera nuevas regulaciones relacionadas con la privacidad de datos, la regulación ambiental y las relaciones laborales durante los próximos cinco años. En general, 89% señala que habrá nuevos requisitos de cumplimiento en al menos una de estas áreas durante el próximo año.

Beth Rose confirma que "la actual administración estadounidense está aumentando la aplicación de la ley y regulando más en todas las áreas, incluidos los aspectos ambientales, sociales y de gobernanza (ESG). Los temas cibernéticos también seguirán creciendo, fundiéndose en uno".

América Latina está experimentando aumentos similares en regulaciones. Larissa Galimberti informa que la Ley General de Protección de Datos de Brasil, que entró en vigor en septiembre de 2020, ha impulsado la actividad de cumplimiento de empresas grandes y pequeñas. La ley otorga derechos sustanciales a los interesados, incluido el acceso a los datos, y exige a todas las empresas que procesan datos que designen un oficial de protección de datos. José Calderón agrega que los requisitos ambientales en áreas como el consumo de agua y la gestión de residuos están creciendo. Estos son "un desafío pero, al mismo tiempo, una oportunidad para responder a las necesidades de los consumidores", afirma.

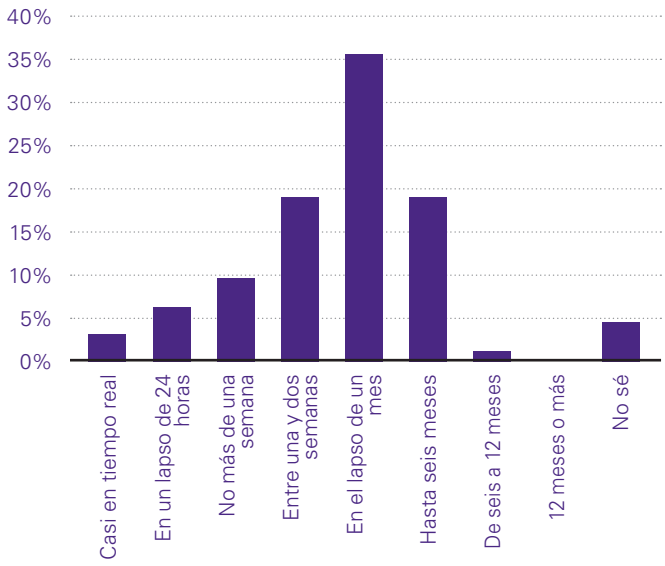
Instantánea de datos III: respuestas lentas, preocupación insuficiente

¿Cuánto tiempo toma, típicamente, identificar un ciberataque o brecha existente en su compañía?



Mediana: aproximadamente 2 semanas

¿Cuánto tiempo toma, típicamente, contener un ciberataque o brecha en su compañía, una vez identificada?



Mediana: aproximadamente 2.5 semanas

Después de un incidente cibernético, "sus datos podrían desaparecer en minutos o segundos. En ese sentido, ninguna velocidad de respuesta es lo suficientemente rápida", observa Ariel Nowersztern, del BID. Del mismo modo, los delincuentes pueden dañar a las empresas de diversas formas al obtener acceso a las redes.

Esto hace que un resultado de la encuesta sea particularmente preocupante: sólo una pequeña proporción de los encuestados considera que sus empresas pueden identificar y luego contener un ciberataque en tiempo real, o incluso en 24 horas.

El tiempo medio para la identificación es mucho más largo (dos semanas) y la contención requiere dos semanas y media adicionales. En general, de acuerdo con la encuesta, generalmente toma alrededor de un mes desde el comienzo de un ciberataque para que la empresa lo contenga.

Los encuestados están sorprendentemente despreocupados: 81% está algo o completamente satisfecho con el tiempo que le toma a su empresa reconocer un ataque tecnológico, y 76% está satisfecho con la velocidad de respuesta.

Nowersztern explica que existen numerosas barreras para una mejor ciberseguridad, incluida la falta de profesionales capacitados y la percepción común de que implica un costo en lugar de una inversión; sin embargo, en última instancia, la actitud despreocupada que muestra la encuesta es el principal obstáculo. "Básicamente", agrega Nowersztern, la solución comienza con "tener un mayor enfoque en la ciberseguridad. Eso es lo que tienes que hacer. Hay herramientas, aunque a veces son difíciles o costosas de implementar".

Los controles integrales de mitigación siguen siendo escasos

Las empresas en Norteamérica se ubican a sí mismas en posición de ventaja comparativa. La mayoría considera que está cumpliendo con los estándares internacionales o que les está yendo bien según los estándares nacionales. Por el contrario, la respuesta más frecuente de la muestra de empresas en América Latina es que, si bien cumplen con las obligaciones legales, no sobresalen en el cumplimiento de los estándares nacionales o internacionales. De hecho, con respecto a la regulación anticorrupción y de lavado de dinero, más de una cuarta parte de las compañías en América Latina no está segura de cumplir plenamente incluso con las regulaciones locales.

Para obtener una imagen más detallada, se analizó qué tan bien están clasificadas las empresas en aspectos individuales de control de fraude (11 áreas), cumplimiento (7 áreas) y ciberseguridad (6 áreas). Una empresa no necesita sobresalir en cada una de estas 24 áreas del ciclo de amenazas. Como afirma Beth Rose, "se supone que el cumplimiento se basa en el riesgo". Demasiado esfuerzo dirigido a áreas de bajo riesgo sería una pérdida inadecuada de recursos. No obstante, los asuntos cubiertos en la encuesta, como los controles financieros y de gestión y la prevención del robo de datos, son lo suficientemente importantes para que la mayoría de las empresas se esfuercen por mejorar su administración.[2]

¿Qué tipo de protección tienen las empresas contra la creciente complejidad del fraude, el cumplimiento y las amenazas a la ciberseguridad?

De acuerdo con distintas evaluaciones, la mayoría tiene un margen sustancial de mejora, especialmente en América Latina, aunque las respuestas de Norteamérica no dan motivo para la complacencia.

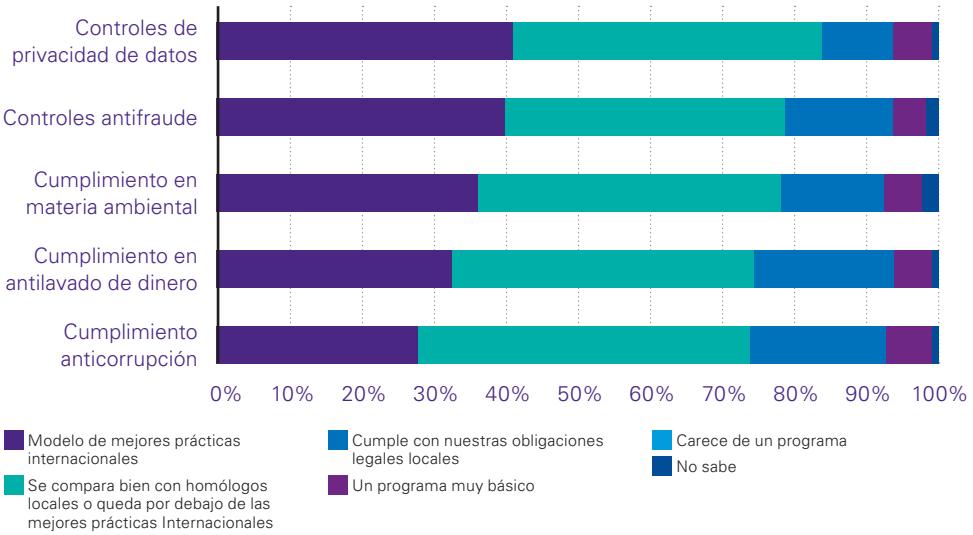
En general, sólo una minoría menciona que su empresa adopta las mejores prácticas internacionales en el cumplimiento de lucha contra la corrupción (18%; cumplimiento ambiental (21%; cumplimiento contra el lavado de dinero (22%; controles antifraude (23%, o controles de privacidad de datos (27%).

2 Las áreas específicas cubiertas son: **para el control del fraude:** controles financieros; seguridad de los activos físicos; seguridad informática; controles de gestión y supervisión; evaluaciones de antecedentes del personal o mecanismos de denuncia; procesos de debida diligencia relacionados con proveedores, socios o clientes; políticas antifraude o matrices de fraude; evaluaciones de riesgo; la formación del personal; planes de respuesta al fraude. **Para el cumplimiento**: prevención del incumplimiento; encontrar e investigar casos de incumplimiento; tomar medidas para mitigarlos; reportar irregularidades a las autoridades para minimizar el riesgo corporativo, multas y sanciones; ajustar y cumplir con los nuevos requisitos reglamentarios de manera oportuna; identificar el riesgo de fraude y cumplimiento entre posibles terceros; adoptar nuevas tecnologías para mejorar el desempeño en las áreas mencionadas. **Para la ciberseguridad**: prevención del robo de datos por parte de piratas informáticos externos; prevención del robo de datos por parte de los empleados; prevención de la pérdida o robo de datos derivados de errores de los empleados; prevención del robo de datos por parte de vendedores, proveedores o socios; prevención de ataques de ransomware; prevención de otros ataques a redes o activos.

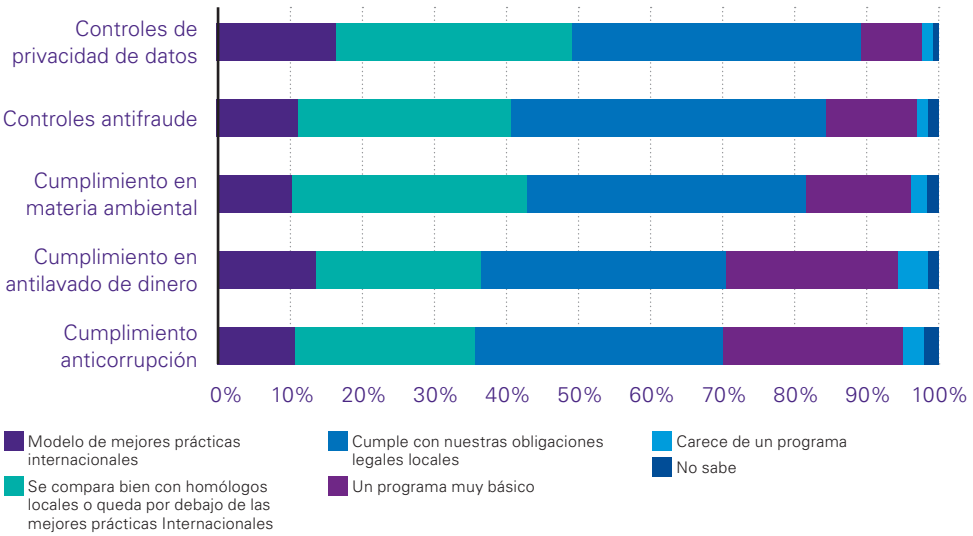
Visto por el lado positivo, para cada control de fraude, consideración de cumplimiento y control de ciberseguridad, entre 85% y 95% califica su negocio como excelente en al menos una de las áreas cubiertas en la encuesta; sin embargo, muy pocos califican el desempeño de su empresa como de alta calidad en todos los ámbitos. Asimismo, se calcula cuántos califican a su organización como excelente al menos en la mitad de las áreas cubiertas en cada parte (a esto se le llama el estándar de "la mitad o más").

En general, sólo 24% afirma que su negocio logra "la mitad o más" del estándar en lo que se refiere a ciberseguridad; 17%, en cuanto a controles de fraude, y sólo 13% en lo tocante a cumplimiento. Además, sólo 4% señala que su empresa logra la mitad o más del estándar en las tres áreas. En resumen, la mayoría de las organizaciones necesitan mejorar la calidad de sus esfuerzos contra el fraude, incumplimiento y los riesgos cibernéticos.

¿Qué tan maduros son los programas de su compañía en las siguientes áreas?
Respuestas de Norteamérica



¿Qué tan maduros son los programas de su compañía en las siguientes áreas?
Respuestas de América Latina



El problema está más extendido en América Latina, donde sólo 20% afirma que su empresa cumple con "la mitad o más" del estándar de ciberseguridad; 11% en lo que se refiere a los controles de fraude, y 9% en cuanto a cumplimiento. El impacto de esta debilidad es evidente en los resultados de otras encuestas; por ejemplo, la muestra señala que las auditorías internas eran responsables de revelar casos de fraude o infracciones de cumplimiento o ciberseguridad en 43 % de las empresas en Norteamérica, pero sólo en 27% de las empresas de América Latina.

De manera similar, otros controles internos sacan a la luz tales problemas en 41% de las empresas en Norteamérica, pero solo en 31% de los casos en América Latina.

Los menores niveles de excelencia en los controles internos también pueden ayudar a explicar los mayores niveles de fraude interno que las empresas en América Latina enfrentan.

La Alta Dirección parece comprender que deben reforzarse las defensas. Alrededor de 65% espera que el gasto en ciberseguridad aumente durante el próximo año; 53% espera un mayor gasto en prevención del fraude, y 44%, en cumplimiento. Menos de 7% en cada caso proyecta que el desembolso disminuya durante los próximos 12 meses.

A medida que las empresas toman estas decisiones de gasto, el consejo más importante que dan nuestros especialistas es no olvidarse de la gente. José Calderón considera que "la formación y retención de buenos colaboradores es una de las cosas más importantes para prevenir el fraude. Esto difunde la cultura adecuada". Beth Rose está de acuerdo en que "el mayor problema es la cultura". Agrega que hacer esto bien requiere no sólo capacitación, sino también cuidar al talento fatigado tras la pandemia. "La gente puede estar llegando a sus límites en un día, o en general, lo que puede llevar a errores o mala conducta. ¿Cómo podemos ayudar a asegurarnos de que las personas estén bien y reciban apoyo? Ese es el asunto principal".

Compañías que cumplen con el estándar "la mitad o más"

Norteamérica

31%	27%	18%
Ciberseguridad	Prevención del fraude	Controles de cumplimiento

América Latina

19%	11%	9%
Ciberseguridad	Prevención del fraude	Controles de cumplimiento

Conclusiones

¿Están las empresas preparadas para la triple amenaza?

Antes de la pandemia, el fraude, el incumplimiento y los ciberataques ya representaban una costosa amenaza para las empresas de las Américas. Ahora, estos se han vuelto más extensos y complejos

De cara al futuro, la Alta Dirección espera otro aumento generalizado del riesgo en esas tres amenazas.

La mayoría de las empresas cuentan con algunas defensas, pero la excelencia integral es poco común. Este es especialmente el caso de América Latina, donde los resultados sugieren, por ejemplo, que la falta de controles efectivos es responsable de niveles más altos de fraude interno. Las empresas en Norteamérica lo están haciendo mejor, pero la mayoría aún se quedan cortas.

Gran parte de las organizaciones están preparadas para invertir más dinero y aumentar el enfoque de liderazgo en estas áreas. En este sentido, se recomienda seguir estos cinco pasos para mitigar la triple amenaza:

01

Establecer el tono correcto por parte del liderazgo

La Alta Dirección y el Consejo deben asegurarse de promover una cultura que fomente la conducta ética y el compromiso con el cumplimiento. Necesitan establecer estándares y procedimientos para prevenir y detectar el fraude, mitigar los riesgos de cumplimiento y ciberseguridad y monitorear el apego a esos estándares. Para respaldarlo, las empresas deben implementar protocolos que aseguren que el Consejo esté informado y puede ejercer una supervisión razonable sobre el cumplimiento y la ética.

02

Llevar a cabo una revisión de riesgo

Las empresas deben implementar un proceso integral de evaluación de riesgos empresariales que incluya fraude y conducta indebida, cumplimiento y amenazas de ciberseguridad y se centre en los riesgos reales, no en los hipotéticos. Esto significa que la Alta Dirección, el Consejo, las áreas de Auditoría Interna, Cumplimiento, Operaciones y otros grupos de interés, deben trabajar juntos para identificar puntos clave de riesgo y diseñar controles para mitigarlos.

03

Comunicarse de manera efectiva

Las compañías deben evaluar los protocolos existentes de capacitación y comunicación para detallar cómo los mensajes sobre riesgos pueden fluir de manera más efectiva a través de la organización. Todas las personas relevantes deben recibir señales claras de la Alta Dirección de que las responsabilidades de control deben tomarse en serio. Para respaldar esto, la capacitación dirigida ayudará a los empleados a comprender su papel en la protección de los activos de la empresa y la mejora de los sistemas de control interno, así como la forma en que sus actividades se relacionan con el trabajo de los demás.

04

Reforzar la detección

El talento es fundamental para descubrir fraudes importantes y faltas de conducta. Las organizaciones en las que la fuerza laboral cree que tiene la responsabilidad de levantar la mano y denunciar las faltas de conducta son las que detectarán el fraude y dichas faltas de manera temprana. En estas empresas, las personas se sienten cómodas alertando y no temen represalias; esperan que la administración sea receptiva. Las compañías deben desarrollar y hacer públicas formas en que colaboradores y terceros relevantes pueden denunciar sospechas de irregularidades y buscar asesoría y aclaraciones sobre las leyes, los reglamentos y los estándares de conducta.

05

Crear una cultura de cumplimiento y rendición de cuentas

Las empresas deben considerar la posibilidad de mejorar sus políticas y protocolos para incluir elementos de cumplimiento y rendición de cuentas que no sean punitivos. Por ejemplo, pueden hacer que los principios éticos, la integridad y el comportamiento formen parte de las evaluaciones de desempeño y proporcionar incentivos o recompensas por logros relacionados con objetivos o metas vinculados con la ética. Esto ayuda a transmitir el mensaje de que las medidas disciplinarias, en casos de fraude e incumplimiento, se aplican de manera constante, independientemente del rango, la antigüedad o la función laboral.

Contactos

Amanda Rigby
Líder de Forensic para Américas
Directora de Asesoría
KPMG en EE.UU.
amandarigby@kpmg.com

Emerson Melo
Socio
KPMG en Brasil
Líder de Forensic para Sudamérica
emersonmelo@kpmg.com.br

Ana López Espinar
Socia
KPMG en Argentina
Líder de Forensic para Sudamérica
ablopez@kpmg.com.ar

Enzo Carlucci
Socio de Riesgos
KPMG en Canadá
ecarlucci@kpmg.ca

Luis Preciado
Socio Líder de Risk Advisory Solutions
KPMG en México
Líder de Forensic para México y Centroamérica
asesoria@kpmg.com.mx

Las declaraciones realizadas en este informe y los estudios de casos relacionados se basan en los resultados de nuestra encuentas y no deben interpretarse como una aprobación de KPMG a los bienes o servicios de las empresas.

Es posible que algunos o todos los servicios descriptos en este documento no estén permitidos para los clientes de auditoría de KPMG y sus afiliados o entidades relacionadas.